REMARKS

In the Official Action mailed **28 July 2006**, the Examiner reviewed claims 49-66. Claims 49-50, 54-56, 60-62, and 66 were rejected under 35 U.S.C. §103(a) as being unpatentable over D. Richard Kuhn (USPN 6,023,765, hereinafter "Kuhn") in view of Sweet et al (USPub 2002/0031230, hereinafter "Sweet"). Claims 51-53, 57-59, and 63-66 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kuhn, in view of Sweet.

Rejections under 35 U.S.C. §103(a)

Independent claims 49, 55, and 61 were rejected as being unpatentable over Kuhn in view of Sweet. Applicant respectfully points out that the present invention is configured to accommodate **multiple database administrators**, which includes **normal database administrators** and **security officers** (see FIG. 1; page 6, lines 9-13; page 6, line 23 to page 7, line 11 of the instant application). Specifically, as illustrated in FIG. 1 (and the associated text), the present invention accommodates a normal database administrators 134 and a security officer 136. Moreover, normal database administrators can perform administrative functions **involving normal users only**, but cannot perform administrative functions involving sensitive users (see page 7, lines 7-9 of the instant application). On the other hand, a security officer can perform administrative functions **involving sensitive users** (see page 7, lines 9-11; and page 8, lines 11-20 of the instant application).

Furthermore, the present invention manages a database system that provides the capability to store sensitive data in encrypted form, while minimizing the number of database administrators who can access the encrypted data (see page 2, line 26 to page 3, line 2 of the instant application). Allowing multiple database administrators to access sensitive data increases the chance that a *rogue database administrator* can obtain the sensitive data. The present invention teaches a special administrator, **the security officer**, who is the **only administrator** allowed to perform administrative functions on sensitive users and sensitive objects (see page

8

7, lines 7-11; page 8, lines 19-20; and page 9, line 4 to page 10, line 3 of the instant application). Hence, in the present invention, it is not possible for normal system administrators to gain access to sensitive data.

Examiner has not demonstrated that the combined invention of Sweet and Kuhn teaches a database system, *wherein the database system includes sensitive users, normal database administrators, and security officers, wherein the security officer is the only administrators that can perform administrative functions involving sensitive users*. First, Examiner presents a special case to rebut Applicant's amendments presented in the Office Action response dated May 12, 2006. However, as Applicant demonstrates below, the Examiner's special case does not teach the present invention. Second, since Examiner's special case does not teach the present invention, Examiner has not demonstrated that the combined invention of Sweet and Kuhn teaches the Applicant's amendments presented in the Office Action response dated May 12, 2006.

(1) Examiner avers that the combined invention of Sweet and Kuhn teaches a security officer that is the only database administrator empowered to perform administrative functions on sensitive users (see page 7-9 of the Office Action dated 07/28/2006). Specifically, Examiner avers that in a special case of the combined invention of Sweet and Kuhn, a security officer can grant only one database administrator to manage the user profile or sensitive user data (see top of page 8 or the Office Action dated 07/28/2006). However, in this special case, the security officer is not the only database administrator empowered to perform administrative functions involving sensitive users. In Examiner's special case there are actually two security officers **as defined by the present invention**. First, the security officer of Sweet and Kuhn can manage user profiles or sensitive users (see Sweet paragraph [0247]), and is therefore the same as a security officer as defined by the present invention. Second, the one database administrator can manage user profiles or sensitive users, and is therefore a security officer as defined by the present

9

invention. Since there are two security officers, but **no normal database administrator**, the Examiner's special case does not teach the present invention.

(2) Applicant maintains the arguments presented in the Office Action response dated May 12, 2006. Examiner rebutted Applicant's amendments from the Office Action response dated May 12, 2006 using the Examiner's special case as described above. However, as Applicant has demonstrated above, the Examiner's special case does not teach the present invention since there are two security officers, and there are no normal database administrators. The purpose of the present invention is *to prevent normal database administrator from gaining access to sensitive users and sensitive data.* In a database system with two security officers (as proposed by the Examiner's special case), but no normal database administrators, the present invention is not needed. However, in a database system where there are multiple normal database administrators, using a security officer is desirable because it can prevent the normal database administrators from performing administrative functions on sensitive users or sensitive data. Examiner's special case does not teach how to do this. Specifically, Examiner's special case does not teach how to prevent a normal database administrator from performing administrative functions involving a sensitive user, while at the same time allowing a security officer to perform administrative functions involving a sensitive user. Thus, the Examiner has not rebutted the amendments presented in the Office Action response dated May 12, 2006.

There is nothing in Kuhn or Sweet, either separately or in concert, which suggests a database system, *wherein the database system includes sensitive users, normal database administrators, and security officers,* wherein the security officers are the only database administrators that can perform administrative functions on the sensitive users.

Accordingly, Applicant has amended independent claims 49, 55, and 61, to clarify that the present invention includes *sensitive users, normal database administrators, and security officers,* wherein the security officers are the only

10

database administrators that can perform administrative functions on the sensitive users. These amendments find support on page 2, line 26 to page 3, line 2; page 6, lines 9-13; page 6, line 23 to page 7, line 11; page 8, lines 11-20; and page 9, line 4 to page 10, line 3 of the instant application.
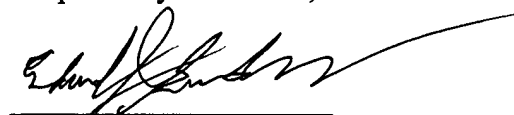
Hence, Applicant respectfully submits that independent claims 49, 55, and 61 as presently amended are in condition for allowance. Applicant also submits that claims 50-54, which depend upon claim 49, claims 56-60, which depend upon claim 55, and claims 62-66, which depend upon claim 61 are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

<u>CONCLUSION</u>

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By

Edward J. Grundler
Registration No. 47,615

Date: 28 August 2006

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1663
FAX: (530) 759-1665
Email: edward@parklegal.com

12